International Privacy Laws

Fair Information Practice Principles *(Click on to FAIR INFORMATION PRACTICES below)*

These widely accepted Fair Information Practice Principles are the basis for many privacy laws in the United States, Canada, Europe and other parts of the world.

"Safe Harbor" Privacy Framework *(Click on to "SAFE HARBOR" PRIVACY FRAMEWORK below)*

Unlike the U.S. approach to privacy protection, which relies on industry-specific legislation, regulation and self-regulation, the European Union relies on comprehensive privacy legislation. The European Directive on Data Protection that went into effect in October 1998, includes, for example, the requirement to create government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The safe harbor - approved by the EU in July of 2000 - is a way for U.S. companies to comply with European privacy laws.

FAIR INFORMATION PRACTICES

These widely accepted Fair Information Practice Principles are the basis for many privacy laws in the United States, Canada, Europe and other parts of the world. The Principles were first formulated by the U. S. Department of Health, Education and Welfare in 1973, and are quoted here from the Organisation for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (available at http://www1.oecd.org/publications/e-book/9302011E.PDF).

Openness

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Collection Limitation

There should be limits to the collection of personal data and any such data should be obtain by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Purpose Specification

The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified as described above, except with the consent of the data subject or by the authority of law.

Data Quality

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, relevant and kept up-to-date.

Individual Participation

An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request is denied and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Security Safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Accountability

A data controller should be accountable for complying with measures which give effect to the principles stated above.

SAFE HARBOR PRIVACY FRAMEWORK:

The European Commission's Directive on Data Protection went into effect in October,1998, and would prohibit the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances

prior approval before personal data processing may begin. As a result of these different privacy approaches, the Directive could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions.

In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework. The Safe Harbor — approved by the EU in July of 2000 — is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the Safe Harbor will assure that EU organizations know that your company provides “adequate” privacy protection, as defined by the Directive.

The U.S. Department of Commerce’s “Safe Harbor” website, http://www.export.gov/safeharbor/index.html, provides the information an organization should need to evaluate, and then join, the Safe Harbor.